PATENT COOPERATION TREATY

From the INTERNATIONAL BUREAU

PCT

NOTIFICATION OF ELECTION

(PCT Rule 61.2)

To:

Assistant Commissioner for Patents
United States Patent and Trademark Office
Box PCT
Washington, D.C.20231
ETATS-UNIS D'AMERIQUE

in its capacity as elected Office

Date of mailing (day/month/year) 06 June 2000 (06.06.00)	
International application No. PCT/US99/22710	**Applicant's or agent's file reference** 1797.014PC02
International filing date (day/month/year) 01 October 1999 (01.10.99)	**Priority date** (day/month/year) 01 October 1998 (01.10.98)
Applicant POOVENDRAN, Raadhakrishnan et al	

1. The designated Office is hereby notified of its election made:

[X] in the demand filed with the International Preliminary Examining Authority on:

01 May 2000 (01.05.00)

[ ] in a notice effecting later election filed with the International Bureau on:

2. The election [X] was

[ ] was not

made before the expiration of 19 months from the priority date or, where Rule 32 applies, within the time limit under Rule 32.2(b).

The International Bureau of WIPO **34, chemin des Colombettes** **1211 Geneva 20, Switzerland**	Authorized officer C. Villet
Facsimile No.: (41-22) 740.14.35	Telephone No.: (41-22) 338.83.38

PATENT COOPERATION TREATY

From the INTERNATIONAL SEARCHING AUTHORITY

To: ROBERT E. SOKOHL
STERNE, KESSLER, GOLDSTEIN, & FOX P.L.L.C.
1100 NEW YORK AVE., N.W. - SUITE 600
WASHINGTON DC 20005-3934

PCT

NOTIFICATION OF TRANSMITTAL OF THE INTERNATIONAL SEARCH REPORT OR THE DECLARATION

(PCT Rule 44.1)

	Date of Mailing *(day/month/year)* 16 FEB 2000
Applicant's or agent's file reference 1797.014PCO2	**FOR FURTHER ACTION** **See paragraphs 1 and 4 below**
International application No. PCT/US99/22710	International filing date *(day/month/year)* 01 OCTOBER 1999
Applicant POOVENDRAN, RAADHAKRISHNAN	

1. [X] The applicant is hereby notified that the international search report has been established and is transmitted herewith.

Filing of amendments and statement under Article 19:
The applicant is entitled, if he so wishes, to amend the claims of the international application (see Rule 46):

When? The time limit for filing such amendments is normally 2 months from the date of transmittal of the international search report; however, for more details, see the notes on the accompanying sheet.

Where? Directly to the International Bureau of WIPO
34, chemin des Colombettes
1211 Geneva 20, Switzerland
Facsimile No.: (41-22) 740.14.35

For more detailed instructions, see the notes on the accompanying sheet.

2. [ ] The applicant is hereby notified that no international search report will be established and that the declaration under Article 17(2)(a) to that effect is transmitted herewith.

3. [ ] **With regard to the protest** against payment of (an) additional fee(s) under Rule 40.2, the applicant is notified that:

[ ] the protest together with the decision thereon has been transmitted to the International Bureau together with the applicant's request to forward the texts of both the protest and the decision thereon to the designated Offices.

[ ] no decision has been made yet on the protest; the applicant will be notified as soon as a decision is made.

4. **Further action(s):** The applicant is reminded of the following:

Shortly after **18 months** from the priority date, the international application will be published by the International Bureau. If the applicant wishes to avoid or postpone publication, a notice of withdrawal of the international application, or of the priority claim, must reach the International Bureau as provided in rules 90 *bis* 1 and 90 *bis* 3, respectively, before the completion of the technical preparations for international publication.

Within **19 months** from the priority date, a demand for international preliminary examination must be filed if the applicant wishes to postpone the entry into the national phase until 30 months from the priority date (in some Offices even later).

Within **20 months** from the priority date, the applicant must perform the prescribed acts for entry into the national phase before all designated Offices which have not been elected in the demand or in a later election within 19 months from the priority date or could not be elected because they are not bound by Chapter II.

Name and mailing address of the ISA/US Commissioner of Patents and Trademarks Box PCT Washington, D.C. 20231	Authorized officer PAUL E. CALLAHAN
Facsimile No. (703) 305-3230	Telephone No. (703) 305-1336

Form PCT/ISA/220 (January 1994)★ *(See notes on accompanying sheet)*

PATENT COOPERATION TREATY

PCT

INTERNATIONAL SEARCH REPORT

(PCT Article 18 and Rules 43 and 44)

Applicant's or agent's file reference 1797.014PCO2	FOR FURTHER ACTION	see Notification of Transmittal of International Search Report (Form PCT/ISA/220) as well as, where applicable, item 5 below.
International application No. PCT/US99/22710	International filing date *(day/month/year)* 01 OCTOBER 1999	(Earliest) Priority Date *(day/month/year)* 01 OCTOBER 1998
Applicant POOVENDRAN, RAADHAKRISHNAN		

This international search report has been prepared by this International Searching Authority and is transmitted to the applicant according to Article 18. A copy is being transmitted to the International Bureau.

This international search report consists of a total of 3 sheets.

[X] It is also accompanied by a copy of each prior art document cited in this report.

1. [ ] **Certain claims were found unsearchable** (See Box I).

2. [ ] **Unity of invention is lacking** (See Box II).

3. [ ] The international application contains disclosure of a **nucleotide and/or amino acid sequence listing** and the international search was carried out on the basis of the sequence listing
   - [ ] filed with the international application.
   - [ ] furnished by the applicant separately from the international application,
     - [ ] but not accompanied by a statement to the effect that it did not include matter going beyond the disclosure in the international application as filed.
   - [ ] transcribed by this Authority.

4. With regard to the **title**,
   - [X] the text is approved as submitted by the applicant.
   - [ ] the text has been established by this Authority to read as follows:

5. With regard to the **abstract**,
   - [ ] the text is approved as submitted by the applicant.
   - [X] the text has been established, according to Rule 38.2(b), by this Authority as it appears in Box III. The applicant may, within one month from the date of mailing of this international search report, submit comments to this Authority.

6. The figure of the **drawings** to be published with the abstract is:

   Figure No. 1

   - [X] as suggested by the applicant.
   - [ ] because the applicant failed to suggest a figure.
   - [ ] because this figure better characterizes the invention.
   - [ ] None of the figures.

International application No.
PCT/US99/22710

Box III TEXT OF THE ABSTRACT (Continuation of item 5 of the first sheet)

A class of distributed key generation (130) and recovery (125) approaches is presented, suitable for group communication systems where the group membership must be tightly controlled. The proposed key generation (130) approach allows entities which may have only partial trust in each other to jointly generate (130) a shared key without the aid of an external third party. The group collectively generates (130) and maintains a dynamic group binding parameter (110), and the shared key is generated (110) using a pseudorandom function (110) using this parameter as a seed. The methods employ distributed algorithms based on fractional keys (FK) (515). The proposed methods allow the members to automatically update the keys in a periodic manner without any assistance from an external third party, and to do so using verifiable secret sharing techniques. The key retreival method (125) does not require the keys to be stored in an external retreival center. Note that many Internet-based applications may have these requirements.

INTERNATIONAL SEARCH REPORT

International application No.
PCT/US99/22710

A. CLASSIFICATION OF SUBJECT MATTER

IPC(6) : H04K 1/00
US CL : 380/283
According to International Patent Classification (IPC) or to both national classification and IPC

B. FIELDS SEARCHED

Minimum documentation searched (classification system followed by classification symbols)

U.S. : 380/259, 380/260, 380/262, 380/265, 380/277, 380/282, 380/283, 380/44, 380/30

Documentation searched other than minimum documentation to the extent that such documents are included in the fields searched

Electronic data base consulted during the international search (name of data base and, where practicable, search terms used)

STN/CAS WEST

C. DOCUMENTS CONSIDERED TO BE RELEVANT

Category*	Citation of document, with indication, where appropriate, of the relevant passages	Relevant to claim No.
X	US 5,625,692 A (HERZBERG et al.) 29 April 1997, col. 5 lines 2-7, col. 8, lines 10-20.	1
A, P	US 5,825,880 A (SUDIA et al.) 20 October 1998, entire document	1-16
A	US 5,708,714 A (LOPEZ et al.) 13 January 1998 entire document	1-16
A	US 5,675,649 A (BRENNAN et al.) 07 October 1997 entire document	1-16
A	US 5,276,737 A (MICALI) 04 January1994 entire document	1-16

☐ Further documents are listed in the continuation of Box C. ☐ See patent family annex.

*	Special categories of cited documents:	"T"	later document published after the international filing date or priority date and not in conflict with the application but cited to understand the principle or theory underlying the invention
"A"	document defining the general state of the art which is not considered to be of particular relevance	"X"	document of particular relevance; the claimed invention cannot be considered novel or cannot be considered to involve an inventive step when the document is taken alone
"E"	earlier document published on or after the international filing date	"Y"	document of particular relevance; the claimed invention cannot be considered to involve an inventive step when the document is combined with one or more other such documents, such combination being obvious to a person skilled in the art
"L"	document which may throw doubts on priority claim(s) or which is cited to establish the publication date of another citation or other special reason (as specified)	"&"	document member of the same patent family
"O"	document referring to an oral disclosure, use, exhibition or other means		
"P"	document published prior to the international filing date but later than the priority date claimed		

Date of the actual completion of the international search 22 DECEMBER 1999	Date of mailing of the international search report 16 FEB 2000
Name and mailing address of the ISA/US Commissioner of Patents and Trademarks Box PCT Washington, D.C. 20231 Facsimile No. (703) 305-3230	Authorized officer PAUL E. CALLAHAN Telephone No. (703) 305-1336

Form PCT/ISA/210 (second sheet)(July 1992)★

PATENT COOPERATION TREATY

From the
INTERNATIONAL PRELIMINARY EXAMINING AUTHORITY

To: ROBERT E. SOKOHL
STERNE, KESSLER, GOLDSTEIN, & FOX P.L.L.C.
1100 NEW YORK AVE., N.W. - SUITE 600
WASHINGTON, DC 20005-3934

PCT

NOTIFICATION OF TRANSMITTAL OF INTERNATIONAL PRELIMINARY EXAMINATION REPORT

(PCT Rule 71.1)

Date of Mailing *(day/month/year)*	08 MAY 2001
Applicant's or agent's file reference: 1797.014PCO2	**IMPORTANT NOTIFICATION**

International application No.	International filing date *(day/month/year)*	Priority Date *(day/month/year)*
PCT/US99/22710	01 OCTOBER 1999	01 OCTOBER 1998

Applicant
POOVENDRAN, RAADHAKRISHNAN

1. The applicant is hereby notified that this International Preliminary Examining Authority transmits herewith the international preliminary examination report and its annexes, if any, established on the international application.

2. A copy of the report and its annexes, if any, is being transmitted to the International Bureau for communication to all the elected Offices.

3. Where required by any of the elected Offices, the International Bureau will prepare an English translation of the report (but not of any annexes) and will transmit such translation to those Offices.

4. **REMINDER**

The applicant must enter the national phase before each elected Office by performing certain acts (filing translations and paying national fees) within 30 months from the priority date (or later in some Offices)(Article 39(1))(see also the reminder sent by the International Bureau with Form PCT/IB/301).

Where a translation of the international application must be furnished to an elected Office, that translation must contain a translation of any annexes to the international preliminary examination report. It is the applicant's responsibility to prepare and furnish such translation directly to each elected Office concerned.

For further details on the applicable time limits and requirements of the elected Offices, see Volume II of the PCT Applicant's Guide.

Name and mailing address of the IPEA/US	Authorized officer
Commissioner of Patents and Trademarks Box PCT Washington, D.C. 20231	TOD R. SWANN James R. Matthews
Facsimile No. (703) 305-3230	Telephone No. (703) 305-1336

Form PCT/IPEA/416 (July 1992)★

PATENT COOPERATION TREATY

PCT

INTERNATIONAL PRELIMINARY EXAMINATION REPORT

(PCT Article 36 and Rule 70)

Applicant's or agent's file reference 1797.014PCO2	**FOR FURTHER ACTION**	See Notification of Transmittal of International Preliminary Examination Report (Form PCT/IPEA/416)
International application No. PCT/US99/22710	International filing date *(day/month/year)* 01 OCTOBER 1999	Priority date *(day/month/year)* 01 OCTOBER 1998
International Patent Classification (IPC) or national classification and IPC IPC(7): H04K 1/00 and US Cl.: 380/283		
Applicant POOVENDRAN, RAADHAKRISHNAN		

1. This international preliminary examination report has been prepared by this International Preliminary Examining Authority and is transmitted to the applicant according to Article 36.

2. This REPORT consists of a total of 3 sheets.

   ☐ This report is also accompanied by ANNEXES, i.e., sheets of the description, claims and/or drawings which have been amended and are the basis for this report and/or sheets containing rectifications made before this Authority. (see Rule 70.16 and Section 607 of the Administrative Instructions under the PCT).

   These annexes consist of a total of 0 sheets.

3. This report contains indications relating to the following items:

   I ☒ Basis of the report

   II ☐ Priority

   III ☐ Non-establishment of report with regard to novelty, inventive step or industrial applicability

   IV ☐ Lack of unity of invention

   V ☒ Reasoned statement under Article 35(2) with regard to novelty, inventive step or industrial applicability; citations and explanations supporting such statement

   VI ☐ Certain documents cited

   VII ☐ Certain defects in the international application

   VIII ☐ Certain observations on the international application

Date of submission of the demand	Date of completion of this report
01 MAY 2000	17 APRIL 2001
Name and mailing address of the IPEA/US Commissioner of Patents and Trademarks Box PCT Washington, D.C. 20231 Facsimile No. (703) 305-3230	Authorized officer TOD R. SWANN James R. Matthews Telephone No. (703) 305-1336

Form PCT/IPEA/409 (cover sheet) (July 1998)★

INTERNATIONAL PRELIMINARY EXAMINATION REPORT

International application No.
PCT/US99/22710

I. Basis of the report

1. With regard to the elements of the international application:*

[X] the international application as originally filed

[X] the description:
pages 1-22, as originally filed
pages NONE, filed with the demand
pages NONE, filed with the letter of _____

[X] the claims:
pages 23-30, as originally filed
pages NONE, as amended (together with any statement) under Article 19
pages NONE, filed with the demand
pages NONE, filed with the letter of _____

[X] the drawings:
pages 1-11, as originally filed
pages NONE, filed with the demand
pages NONE, filed with the letter of _____

[X] the sequence listing part of the description: NONE, as originally filed
pages NONE, filed with the demand
pages NONE, filed with the letter of _____

2. With regard to the language, all the elements marked above were available or furnished to this Authority in the language in which the international application was filed, unless otherwise indicated under this item.
These elements were available or furnished to this Authority in the following language _____ which is:

[ ] the language of a translation furnished for the purposes of international search (under Rule 23.1(b)).

[ ] the language of publication of the international application (under Rule 48.3(b)).

[ ] the language of the translation furnished for the purposes of international preliminary examination (under Rules 55.2 and/or 55.3).

3. With regard to any nucleotide and/or amino acid sequence disclosed in the international application, the international

[ ] contained in the international application in printed form.

[ ] filed together with the international application in computer readable form.

[ ] furnished subsequently to this Authority in written form.

[ ] furnished subsequently to this Authority in computer readable form.

[ ] The statement that the subsequently furnished written sequence listing does not go beyond the disclosure in the international application as filed has been furnished.

[ ] The statement that the information recorded in computer readable form is identical to the written sequence listing has been furnished.

4. [X] The amendments have resulted in the cancellation of:

[X] the description, pages NONE

[X] the claims, Nos. NONE

[X] the drawings, sheets/fig NONE

5. [ ] This report has been drawn as if (some of) the amendments had not been made, since they have been considered to go beyond the disclosure as filed, as indicated in the Supplemental Box (Rule 70.2(c)).**

** Replacement sheets which have been furnished to the receiving Office in response to an invitation under Article 14 are referred to in this report as "originally filed" and are not annexed to this report since they do not contain amendments (Rules 70.16 and 70.17).*

***Any replacement sheet containing such amendments must be referred to under item 1 and annexed to this report.*

INTERNATIONAL PRELIMINARY EXAMINATION REPORT

International application No.
PCT/US99/22710

V. Reasoned statement under Article 35(2) with regard to novelty, inventive step or industrial applicability; citations and explanations supporting such statement

1. statement

Novelty (N)	Claims	2-14	YES
	Claims	1, and 15-16	NO
Inventive Step (IS)	Claims	2-14	YES
	Claims	1, 15-16	NO
Industrial Applicability (IA)	Claims	1-16	YES
	Claims	NONE	NO

2. citations and explanations (Rule 70.7)

Claims 1 and 15-16 lack novelty under PCT Article 33(2) and lack an inventive step under PCT Article 33(3) as being anticipated by and being obvious over Herzberg et al. US Patent 5,625,692 April 27, 1997.

Herzberg teaches a method of generating and managing shared keys for a plurality of members of a cluster in col. 5 lines 2-7 and col. 8 lines 10-20.

Claims 2-14 meet the criteria set out in PCT Article 33(2)-(4), because the prior art does not teach or fairly suggest the method of claim 1 with the additional feature of generating a random initial one time pad as found in claim 2 and the generation steps of claims 3-14 utilizing the specific variables mentioned at the algorithm steps as detailed in the claims.

---------- NEW CITATIONS ----------
NONE